UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

MICHAEL WAMBOLD and ROBERT GUPTILL, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. RTA MEDIA HOLDINGS, LLC d/b/a RACING AMERICA, Defendant.	**Case No.: 1:25-cv-96** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Michael Wambold and Robert Guptill ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against defendant RTA Media Holdings, LLC d/b/a Racing America ("Racing America" or "Defendant"). Racing America owns and manages a video streaming website at https://www.racingamerica.tv/ (the "Website"). On the Website, Defendant utilized tracking tools to intercept and disclose consumers' search terms, video watching information, and personally identifiable information (collectively, "Sensitive Information") without seeking or obtaining consumers' consent (the "Tracking Tools"). The Website's use of the Tracking Tools resulted in violations of the Video Privacy Protection Act ("VPPA"), state and federal wiretap statutes, and invasions into consumers' privacy. Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who subscribed to the Website and subsequently watched pre-recorded video content on the Website.

2. The Website offers users the ability to sign up for free newsletters by providing their email addresses, or pay money to obtain a membership to Racing America's streaming service (the "Subscribers").

3. A monthly subscription to the Website costs $14.99 USD a month or $109.99 USD a year.[1]

4. This subscription unlocks access to a large collection ranging from pavement short track racing, to original NASCAR Cup Team content, to behind the scenes exclusives.[2]

5. In short, the Website's raison d'etre is providing access to and delivering pre-recorded video content.

6. Defendant chose to work with Vimeo, Inc. ("Vimeo") to host the Website's videos and provide the streaming technology so that Subscribers could digitally access Defendant's video content.

7. Defendant made use of Vimeo's "over the top" ("OTT") platform, which allows video content providers, like Defendant, to "send content over a high-speed internet connection . . . [so] users can access the content they want straight from the creator, without having to through an intermediary . . . ."[3]

---

[1] *Racing America Subscription*, RACING AMERICA, https://www.racingamerica.tv/checkout/premium-membership-4/purchase (last visited Jan. 8, 2025).

[2] *Subscribe to RacingAmerica.tv*, RACING AMERICA, https://offer.racingamerica.com/?__hstc=26610594.5e03eeb036bc7e9a44bef0be077f7705.1735658866886.1735753080112.1735762732883.3&__hssc=26610594.1.1735762732883&__hsfp=1154299380&_gl=1*pdvtkp*_ga*MTU1NTUzNDUzNS4xNzM1NjU4ODY1*_ga_T7K4NMX5XG*MTczNTc2MjcyOC40LjEuMTczNTc2MjcyOS4wLjAuMA..#:~:text=From%20pavement%20short,in%20special%20offers (last visited Jan. 8, 2025).

[3] *Create an OTT platform*, VIMEO, https://vimeo.com/ott (last visited Jan. 8, 2025).

8. In all instances, the web watching of videos on the Website is tracked by Defendant as a result of its decision to place the Tracking Tools on each individual page containing video content on the Website.

9. Defendant does not disclose that Subscribers' Sensitive Information, including personal identifying information ("PII"),[4] would be captured by the Tracking Tools, and then transmitted to third parties.

10. The Website does not inform Subscribers that their Sensitive Information will be exposed, available, and readily usable by any person of ordinary technical skill who receives that data.

11. At no point during or after the subscription sign up process – or anywhere on the Website for that matter – does Defendant seek or obtain consent for the sharing of Subscribers' Sensitive Information, which Defendant surreptitiously gathered through the use of the Tracking Tools that it chose to employ on the Website.

Video Privacy Violations

12. In today's data driven world, a company's data sharing policies for a service or subscription are important factors for individuals to consider in deciding whether to provide personal information to that service or commit to a subscription.

13. Congress has recognized the immediate and irreversible harm caused by associating and disclosing a person's personally identifiable information in conjunction with their video watching information.

[4] 18 U.S.C. § 2710(a)(3) ("includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider").

14. Congress' enactment of the VPPA, and its continued endorsement of the statute, supports that recognition. The VPPA prohibits video tape service providers,[5] such as Defendant, from sharing subscribers' PII tied to the title, description, or subject matter of pre-recorded audio video material[6] without valid consent.[7]

15. Congress made clear that the harm to individuals impacted by VPPA violations occurs the moment, and each time, a consumer's information is shared.

16. Defendant purposefully implemented and utilized Meta, Inc.'s ("Facebook" or "Meta") tracking pixel (the "Pixel," discussed and defined herein) to track Subscribers' activity on the Website and disclose that information, including Subscribers' PII, to Facebook to gather valuable marketing data. The Pixel could not be placed on the Website without steps taken directly by or on behalf of Defendant.

17. Because of Racing America's decision to employ the Pixel and because it chose to employ the Pixel on its video content on the Website, a Subscriber's PII is shared *the moment* the Subscriber requests video materials.[8]

18. Defendant does not seek and has not obtained consent from Subscribers to utilize the Pixel to track, share, and exchange their Sensitive Information, including their PII, with Facebook.

---

[5] 18 U.S.C. § 2710(a)(4).
[6] 18 U.S.C. § 2710(b)(2)(D)(II).
[7] 18 U.S.C. § 2710.
[8] As defined by the VPPA, protected "personally identifiable information" includes information which identifies a person as having "*requested* or obtained" video materials. *See* 18 U.S.C. § 2710(a)(3). When a website user clicks a link leading to a video, the user "requests" authorization to access the material from the website's server and, if authorized, the server then sends the data to the user. *See How the web works*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited Jan. 8, 2025).

19. Subscribers of the Website have been harmed as a result of violations of the VPPA. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Pixel from the Website, or (ii) add adequate notices and obtain the appropriate consent from Subscribers.[9]

Wiretap Violations

20. Federal and state legislatures addressed citizens' privacy expectations when communicating with parties over wired communications.

21. Congress passed the Federal Wiretap Act, which prohibits the unauthorized interception of electronic communications.

22. Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701 *et seq.* "prohibits the interception of wire, electronic, or oral communications, which means it is unlawful to acquire those communications using a device."[10]

23. Defendant purposefully implemented and utilized the Pixel and other Tracking Tools to intercept and read Subscribers' search terms and disclose the location and content of webpages visited by Subscribers. The Website does not provide notice of or obtain consent as to such practices.

24. Subscribers of the Website, such as Plaintiffs, have an interest in maintaining control over their Sensitive Information, as well as an interest in preventing their misuse.

---

[9] Website owners like Racing America also have the option to anonymize the video's title within the URL or encrypt the video title using hashing, as described by Facebook. *See Advanced Matching*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching#security (last visited Jan. 8, 2025); *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools (last visited Jan. 8, 2025) ("When using a Meta image pixel or other Meta Business Tools, you or your service provider must hash [personally identifiable information] in a manner specified by us before transmission.").

[10] *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

25. Subscribers of the Website have been harmed by Defendant, resulting in violations of the Federal Wiretap Act and WESCA. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Tracking Tools from the Website, or (ii) add, and obtain, appropriate consent from Subscribers.

26. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of Subscribers of the Website for violations of the VPPA, 18 U.S.C. § 2710; violations of the Federal Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e); and violations of WESCA, 18 Pa. C.S. § 5701 *et seq.*

PARTIES

27. Plaintiff Michael Wambold is, and has been at all relevant times, a citizen of Pennsylvania who resides in Brodheadsville, Pennsylvania. Plaintiff Wambold became a subscriber to the Website in or around 2023. Plaintiff Wambold used the Website for its intended purposes to access and view video content available to Plaintiff Wambold through the Website. One such video was "PPV 2024 Turkey Derby All Access at Wall Stadium." Plaintiff Wambold used a Chrome internet browser to view Defendant's video content while logged into his Facebook account on the same browser. Plaintiff Wambold's Facebook profile includes identifiable information, including his name, where he lives, and personal photos. Plaintiff Wambold did not consent, agree, authorize, or otherwise permit Defendant to disclose his Sensitive Information to third parties. Plaintiff Wambold was not provided with written notice that Defendant discloses its Subscribers' Sensitive Information, or any means of opting out of the disclosures of their Sensitive Information. Still, Defendant knowingly disclosed Plaintiff Wambold's Sensitive Information to third parties. Defendant has violated Plaintiff Wambold's right to privacy under the VPPA, the

Federal Wiretap Act, and WESCA. If not for these violations of his privacy, Plaintiff Wambold would continue his use of the Website.

28. Plaintiff Robert Guptill is, and has been at all relevant times, a citizen of Maine who resides in South Paris, Maine. Plaintiff Guptill became a subscriber to the Website in or around 2023. Plaintiff Guptill used the Website for its intended purposes to access and view video content available to Plaintiff Guptill through the Website, including videos from events at the Oxford Plains Speedway. Plaintiff Guptill used a Chrome internet browser to view Defendant's video content while logged into his Facebook account on the same browser. Plaintiff Guptill's Facebook profile includes identifiable information, including his name, where he lives, and personal photos. Plaintiff Guptill did not consent, agree, authorize, or otherwise permit Defendant to disclose his Sensitive Information to third parties. Plaintiff Guptill was not provided with written notice that Defendant discloses its Subscribers' Sensitive Information, or any means of opting out of the disclosures of their Sensitive Information. Still, Defendant knowingly disclosed Plaintiff Guptill's Sensitive Information to third parties. Defendant has violated Plaintiff Guptill's right to privacy under the VPPA and the Federal Wiretap Act. If not for these violations of his privacy, Plaintiff Guptill would continue his use of the Website.

29. Defendant RTA Media Holdings, LLC d/b/a Racing America is a motorsports media company that focuses on digital content and direct-to-consumer services. Defendant owns and operates Racing America TV, which offers live and on-demand grassroots racing, Cup Team news and content, and behind the scenes access to all things racing. Defendant is headquartered in Concord, North Carolina.

JURISDICTION AND VENUE

30. The District Court for the Middle District of North Carolina has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the

aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from at least one Defendant. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the Video Privacy Protection Act, 18 U.S.C. § 2710, and the Federal Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e).

31. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in North Carolina, and Defendant derives revenue in the State of North Carolina, including Defendant's revenue generated from its management over the Website, including the revenue sharing, advertising sales, etc. that Defendant derives from the Website.

32. Venue is proper in the Middle District of North Carolina pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and Defendant conducts substantial business operations in this District. In connection with the Website, the video content, the hosting of media accessible to Subscribers, and associated coding, all claims originate and arise out of the Defendant's business operations in this District.

COMMON FACTUAL ALLEGATIONS

I. Legislative Background

A. The Video Privacy Protection Act

33. The history of the VPPA begins in 1988, when a Washington-based newspaper published a profile of Supreme Court nominee, Judge Robert H. Bork "based on the titles of 146 films his family had rented from a video store." S. Rep. No. 100-599 at 5 (1988). Senators took to the floor to denounce the invasion of privacy, with Senator Patrick Leahy noting that:

> In an era of interactive television cables, the growth of computer checking and check-out counters . . . all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch . . . I think it is something that we have to guard against.

Id. at 5-6.

34. Congress believed that these "information pools" created privacy interests that directly affected the ability of people to freely express their opinions, join in association with others, or enjoy the general freedoms and independence protected by the Constitution. *Id.* at 7.

35. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id.* at 7-8 (statements of Sens. Simon and Leahy, respectively).

36. Senator Simon lamented that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* at 6-7.

37. As a result, the VPPA was drafted to "give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives" by prohibiting "unauthorized disclosures of personal information held by video tape providers." *Id.* at 6.

38. The VPPA regulates the disclosure of information about consumers' consumption of video content, imposing specific requirements to obtain consumers' consent to such disclosure. Under the statute, for each violation of the statute, a court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief, and attorney's fees.

39. The statutory damages were deemed "necessary to remedy the intangible harm caused by privacy intrusions." *Id.* at 8.

40. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow

consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

41. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy stated that "[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[11]

42. This application of the VPPA to modern video sources, such as websites, has been confirmed by various courts across the country.[12]

43. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

44. Congress wanted to ensure that any transaction between consumer and VTSP involving a request or procurement of specific video materials or video services would be protected. In short, the language is broad enough to encompass digital as well as physical transactions, so long as the transaction includes the defined and prohibited information.

---

[11] See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, *available at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Jan. 8, 2025).

[12] *See, e.g., Sellers v. Bleacher Report, Inc.*, 2023 U.S. Dist. LEXIS 131579, at *15-18 (N.D. Cal. July 29, 2023) (VPPA sufficiently applied to sports news website); *Jackson v. Fandom, Inc.*, 2023 U.S. Dist. LEXIS 125531, at *6 (N.D. Cal. July 20, 2023) (VPPA applies to gaming and entertainment website); *Louth v. NFL*, 2022 U.S. Dist. LEXIS 163706, at *11-12 (D.R.I. Sep. 12, 2022) (holding VPPA applied to NFL's videos accessible through mobile app).

45. The VPPA defines personally identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3).

46. A video tape service provider ("VTSP") is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

47. VTSPs are not required to deal exclusively in audio visual content; rather, audiovisual content need only be part of the provider's book of business. *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 547-48 (2d Cir. 2024).

48. A consumer is "any renter, purchaser, or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1).

49. In interpreting the definition of VTSPs, the *Salazar* Court also reasoned that 'consumer' should be understood to encompass a renter, purchaser, or subscriber of *any* of the provider's 'goods or services'—audiovisual or not. *Salazar*, 118 F.4th at 548-49.

50. Defendant here is a video service provider as it provided pre-recorded audio-visual materials to Plaintiffs and Class Members on its Website.

51. The relationship between Plaintiffs and Defendant is precisely the type of relationship contemplated by the VPPA.

52. In this case, Plaintiffs' PII was knowingly and systematically disclosed to Facebook, without obtaining their consent.

B. The Federal Wiretap Act

53. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor

telephonic communications."[13]

54. The Wiretap Act primarily concerned the government's use of wiretaps but Congress grew concerned that technological advancements like "large-scale mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing" were rendering the Wiretap Act out of date.[14] Thus, in 1986, Congress amended the Wiretap Act through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[15]

55. The ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third party processing of data and files.[16]

56. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

57. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is

---

[13] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022).
[14] Senate Rep. No. 99-541, at 2 (1986).
[15] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022).
[16] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

58. While communicating with Defendant on the Website through their viewing choices, Subscribers had the contents[17] of their communications with Defendant intercepted by third parties via the Tracking Tools.

59. Defendant purposefully included the Tracking Tools on the Website to intercept Plaintiffs' communications and redirect them to third parties to improve the effectiveness of its advertising and marketing.

60. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant to third parties.

C. The Pennsylvania Wiretapping and Electronic Surveillance Control Act

61. Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701 *et seq.* has its roots in the common law right to privacy, which protects citizens' "protectable interest in their private information and . . . the sanctity of their communications."[18]

62. WESCA operates in conjunction with and as a supplement to the Federal Wiretap Act, which allows states to "grant greater, but not lesser, protection than that available under federal law."[19] WESCA does so.

---

[17] The contents of Plaintiffs' and users' communications include: 1) search terms submitted to the site; 2) the location and contents of webpages visited by users; and, 3) the PII discussed in Section IIIA.

[18] *Petris v. Sportsman's Warehouse, Inc.*, No. 2:23-CV-1867, 2024 WL 2817530 (W.D. Pa. June 3, 2024).

[19] *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

63. WESCA prohibits: (1) the intentional interception of wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom to another person; and (3) the intentional use of the contents of any wire, electronic or oral communication, or evidence derived therefrom. 18 Pa. C.S. § 5703(a).

64. "Intercept" is defined as: "Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 19 Pa. C.S. § 5702.

65. WESCA defines electronic communication as: "Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature . . . ." Id.

66. Under WESCA, a court may award actual damages (but not less than liquidated damages computed at the rate of $100 a day for each violation of the statute, or $1,000, whichever is higher), punitive damages, equitable relief, and attorney's fees.

67. In this case, Plaintiffs' data—their PII and video watching information—constitutes electronic communications with Defendant.

68. Plaintiffs' electronic communications with Defendant were intentionally intercepted by Defendant through the Tracking Tools that Defendant employed on the Website.

69. Plaintiffs' electronic communications were subsequently disclosed to third parties.

70. Defendant used the contents of Plaintiffs' electronic communications with the Website, intercepted and processed by third parties, to target Plaintiffs with advertising.

71. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Defendant.

72. Defendant acted with the intent to intercept, disclose, and use Plaintiffs' protected, private information for their economic benefit through the monetization of the information via targeted advertising and other means.

II. Defendant Controls the Website

A. Racing America Owns and Manages the Website

73. Racing America maintained control over the Website.

74. While Vimeo provided the underlying technology for the Website and video streaming services, Racing America maintained control over the relevant portions of the Website.

75. RTA Media Holding's ownership of the Website is reflected in its Privacy Policy: "This is the Privacy Policy of RTA Media Holdings, LLC (hereafter referred to as "us" or "we"). This Privacy Policy describes how your personal information is collected, used, and shared when you use our streaming service, RacingAmerica.TV, through our website (https://www.racingamerica.tv/) or any of our branded apps (together, the "Service")."[20]

76. Racing America's management and control does not end there. The Privacy Policy also states: "For more information about our privacy practices, if you have questions, or if you would like to make a complaint, please contact us by using our form or by mail using the details provided below: RTA Media Holdings, LLC Attn: General Counsel PO Box 77268 Charlotte, NC 28271[.]"[21]

B. Racing America Manages the Relevant Portions of the Website

[20] *Privacy Policy*, RACING AMERICA, https://www.racingamerica.com/privacy-policy#:~:text=This%20is%20the,this%20Privacy%20Policy (last visited Jan. 8, 2025).
[21] *Id.*

77. OTT website owners have control over and choose which videos to upload and make available to their Subscribers.[22]

78. OTT website owners also have control over how subscriptions work, including which videos are unlocked by subscriptions and become deliverable to Subscribers.[23]

79. Vimeo provides instructions to OTT website owners, like Defendant, on how to add metadata to help users discover new and relevant video content or otherwise search within the OTT website to find videos to watch.[24]

80. Vimeo recommends, for example, naming videos to improve search engine optimization.[25]

81. Vimeo establishes that when a video is added to an OTT website by its owner or operator, the video is named after the digital file uploaded by default.[26]

82. The responsibility for providing clear titles to videos falls to the OTT website owner, which in turn, is used "to form the URL where the video lives."[27]

83. OTT website owners are given an additional opportunity to "rename a video or collection . . . URL [to] something relevant . . . ."[28]

---

[22] *See Uploading videos on Vimeo OTT*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426966892561-Uploading-videos-on-Vimeo-OTT (last visited Jan. 8, 2025).
[23] *See Creating and Editing a Subscription*, VIMEO, *https://help.vimeo.com/hc/en-us/articles/12427127095441-Creating-and-editing-a-subscription-product-on-Vimeo-OTT* (last visited Jan. 8, 2025).
[24] *See Add metadata to my Vimeo OTT videos for discovery*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427018284945-Add-metadata-to-your-Vimeo-OTT-videos-for-discovery (last visited Jan. 8, 2025).
[25] *See Optimize your Vimeo OTT site for search engines (SEO)*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426994162961-Optimize-your-Vimeo-OTT-site-for-search-engines-SEO (last visited Jan. 8, 2025).
[26] *Id.*
[27] *Id.*
[28] *Id.*

84. OTT website owners must take affirmative steps to add detailed URLs to their OTT websites.

85. Defendant undertook these steps. Racing America added detailed URLs to the Website.

86. Vimeo gives OTT website owners the ability to add metadata to their videos "so that [their] customers can easily discover related content they might enjoy. It also allows [OTT website owners] to make it easier for viewers to find [OTT website owners'] content via search or other parameters."[29]

87. The metadata added to videos by OTT website owners can include: information about the video, like content tags that "describes the specific video"; genres; cast; crew; release date; ratings; advisories, if the video contains offending content; and advanced or custom metadata created by the OTT website owners.

88. OTT website owners must take affirmative steps to add metadata to their OTT websites.

89. Racing America undertook these steps. Racing America added metadata to the Website.

90. Vimeo informs OTT website owners – those which provide content to stream on Vimeo's OTT platforms – that Vimeo merely provides support for OTT website owners "adding conversion tracking Pixels from services like Facebook, X (formerly Twitter), or Adwords . . . ."[30]

---

[29] *Add metadata to my Vimeo OTT videos for discovery*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427018284945-Add-metadata-to-your-Vimeo-OTT-videos-for-discovery (last visited Jan. 8, 2025).

[30] *Add tracking pixels to your Vimeo OTT checkout page*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427502043409-Add-tracking-pixels-to-your-Vimeo-OTT-checkout-page (last visited Jan. 8, 2025).

91. Vimeo explains that "[a] pixel tracks certain events (like when someone makes a purchase through your site, etc.); when the events you're tracking are triggered, the pixel sends the data over to your analytics."[31]

92. Vimeo adds that after an OTT website owner installs a tracking pixel on their OTT website, the intercepted data is viewable on the OTT website owner's account with each pixel's platform.[32]

93. Vimeo then provides instructions to OTT website owners, like Racing America, on how to add the Pixel to their OTT Websites. OTT website owners choose whether to add tracking tools, like the Pixel, to the Vimeo-associated websites.

94. To do so, OTT website owners must first create a Pixel on Facebook's platform; and add that Pixel ID to Vimeo's tracking integration.[33] Then, the OTT website owner must attach the tracking pixel to their Associated Product in their OTT website (or otherwise select "All Products").[34] Finally, the OTT website owner must save these settings.

95. Vimeo advises OTT website owners that the Pixel tracks the following events by default: PageView, InitiateCheckout, Purchase, and Complete Registration.[35]

96. Racing America undertook the steps necessary to add the Pixel to its Website. Racing America also made use of the Pixel SubscribedButtonClick event. Racing America did not accept the default events. Instead, Racing America programmed the Pixel to collect additional information when subscribers click specific buttons, such as to request videos. *See* Section III(A).

---

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

97. Racing America controlled its Privacy Policy and cookie notifications on the Website.

98. While Vimeo provides a "simple cookie consent banner" for OTT websites, Vimeo informs OTT website owners that "[c]ertain sites may be subject to further regulations depending on their purpose, content, and user base. It is up to the site owner to determine if a site requires a more robust cookie consent banner."[36]

99. For those that want more robust cookie consent banners, OTT website owners are offered a chance to integrate "with a third-party solution to ensure legal compliance."[37]

100. Similarly, "[a]s the operator of [its] streaming service, [OTT website owners, like Racing America,] must provide [their] users with a transparent notice of how [they] handle[] their personal information, commonly known as a 'privacy policy.'"[38]

101. Vimeo provides OTT website owners with a "template that already includes the most common points of collection and uses of data for OTT streaming services." Vimeo makes clear, however, that it "makes no representation about the sufficiency or legality of the templated privacy policy" and that OTT website owners "should change the default languages depending on [their] uses of data, additional collection points, and the laws to which [their] organization[s] may be subject."[39]

---

[36] *Setting up my Vimeo OTT site's cookie consent banner*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426990708241-Setting-up-your-Vimeo-OTT-site-s-cookie-consent-banner (last visited Jan. 8, 2025).
[37] *Id.*
[38] *Creating a Privacy Policy for your Vimeo OTT* site, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426965771665-Creating-a-Privacy-Policy-for-your-Vimeo-OTT-site (last visited Jan. 8, 2025).
[39] *Id.*

102. Thus, Racing America was responsible for notifying Subscribers, and obtaining their consent, yet failed to do so in accordance with the VPPA and other federal and state laws.

III. The Website and the Tracking Tools

103. On the Website, Defendant utilized Tracking Tools, including those created by Facebook, Google, Twitter, Bing, and Vimeo (collectively, the "Tracking Entities"), to intercept and disclose Subscribers' Sensitive Information without seeking or obtaining Subscribers' consent.

A. The Facebook Pixel

104. Facebook offers the Pixel to web developers for the purpose of monitoring user interactions on their websites, which can then be shared with Facebook.

105. The Pixel is a marketing tool that can only be added to a webpage by website developers. A website operator must sign up for a business account or link a related Facebook account with its Pixel, and then add code to the website to make use of the Pixel.[40]

106. As Facebook notes, the Pixel must be added to each individual page that a website owner wishes to be tracked.[41]

107. Here, as discussed in Section II(B), Defendant took steps to add the Pixel to the Website via the Vimeo platform.

---

[40] *Set up and install the Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Jan. 8, 2025).

[41] *Get Started*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/get-started/ (last visited Jan. 8, 2025) ("To install the Pixel, add its base code . . . on every page where you will be tracking website visitor actions.").

108. The Pixel is employed by Racing America to gather, collect, and then share user information with Facebook.[42] Receiving this information enables Facebook and the web developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[43] The sharing of Subscribers' Sensitive Information benefits Racing America by improving the effectiveness of advertising targeted at Racing America Subscribers. Studies have shown that personalization in digital marketing through targeted and dynamic advertising can boost revenue by 15%.[44]

109. Website owners and operators can choose to use the Pixel to share both user activity (including video watching activity) and user identity with Facebook. Here, the Website shares both.

110. The harvested data can improve advertising by pinpointing audience demographics by interests, gender, or location and finding the people who are most likely to take action and view content.[45]

111. The Sensitive Information harvested by Racing America provides similar, if not more, data, including the titles of videos, whether through search terms, webpage URLs, parameters, or metadata, in addition to their Facebook profile data.

112. The owner or operator of a website holds the decision-making authority over the

---

[42] The Facebook Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited Jan. 8, 2025).

[43] *See Meta Pixel*, FACEBOOK, https://www.facebook.com/business/tools/meta-pixel (last visited Jan. 8, 2025).

[44] Wilson Lau, *What is Targeted Advertising?*, ADROLL BLOG (June 30, 2024), https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Benefits%20of%20Targeted%20Advertising,-1.%20Deliver%20a%20higher.

[45] *See Audience ad targeting*, FACEBOOK, https://www.facebook.com/business/ads/ad-targeting (last visited Jan. 8, 2025).

placement of the Pixel on its site, as well as whether or not any of the data within the Pixel transmission should be "hashed" (a form of encryption).

1. Defendant Implemented the Facebook Pixel on the Website

113. To activate and employ a Facebook Pixel, a website owner must first sign up for a Facebook account, where specific "business manager" accounts are provided the most utility for using the Pixel.[46] For instance, business manager accounts can: (i) create and utilize more simultaneous Pixels, (ii) manage multiple Facebook Ad Accounts and Pages from a centralized interface, (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) build custom audiences for multiple ad campaigns, and (v) eliminate privacy concerns related to using a personal profile for business purposes.[47]

114. To add an operational Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Pixel during the creation and setup of the Pixel.[48]

115. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,[49] and must connect the Pixel to a Facebook Ad account.[50]

116. To add the Pixel to its OTT website, the website operator must follow the

---

[46] *How to set up your Meta Pixel with a business portfolio*, FACEBOOK, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited Jan. 8, 2025).

[47] Jacqueline Zote, *A step-by-step guide on how to use Facebook Business Manager*, SPROUTSOCIAL (June 14, 2021), https://sproutsocial.com/insights/facebook-business-manager/.

[48] *Id.*; *see also* Ivan Mana, *How to Set Up & Install the Facebook Pixel*, YOUTUBE (Feb. 4, 2022) https://www.youtube.com/watch?v=ynTNs5FAUm8.

[49] *Add people to your Meta Pixel in Meta Business Suite or Business Manager*, FACEBOOK https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited Jan. 8, 2025).

[50] *Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/622772416185967 (last visited Jan. 8, 2025).

instructions provided by Vimeo discussed, *supra*, in Section II(B).

117. After following these steps, a website operator can start capturing and sharing information using the Pixel.

118. A Pixel cannot be placed on a website by a third-party. It must be placed directly by or on behalf of the site owner. Racing America did so.

2. The Pixel as a Tracking Tool

119. Once the Pixel is set and activated, it can begin collecting and sharing user activity data as instructed by the website owner.

120. When a Facebook user logs onto Facebook, a "c_user" cookie – which contains a user's non-encrypted Facebook User ID number ("UID") – is automatically created and stored on the user's device for up to a year.[51]

121. This means that for Subscribers to the Website who are also Facebook users, their PII is certain to be shared. Their PII is automatically bundled with their web watching history and disclosed to Facebook when visiting a page with an active Pixel, including the home page.

122. While the process to determine what information is being collected by the Pixel from a user is admittedly complicated, the recipient of the Pixel's transmissions receives the information in a clear and easy to understand manner.

123. The seemingly complex data, such as the long URLs included in the Pixel's transmission, is "parsed," or translated into an easier to read format, such that the information is legible.

124. For example, an embedded URL in a Pixel HTTP Request may look like an indecipherable code, as depicted below:

---

[51] *Cookies Policy: What are cookies, and what does this policy cover?*, FACEBOOK (Dec. 12, 2023) https://www.facebook.com/policy/cookies/ (last visited Jan. 8, 2025).

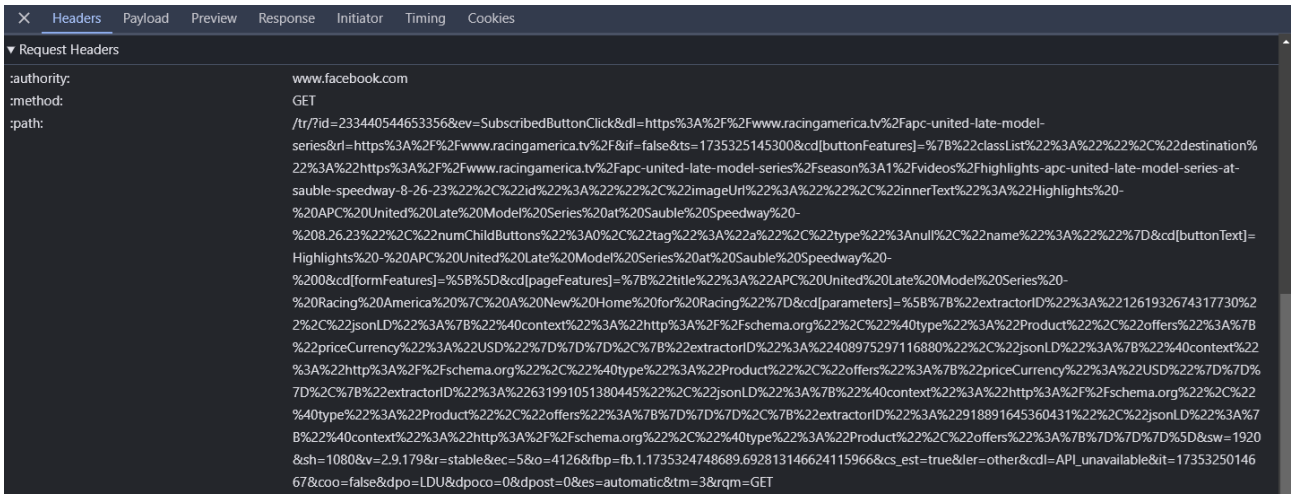

Figure 1 1 - Sample Pixel Request URL

125. However, these URLs are designed to be "parsed" into easy-to-digest pieces of information, as depicted below:

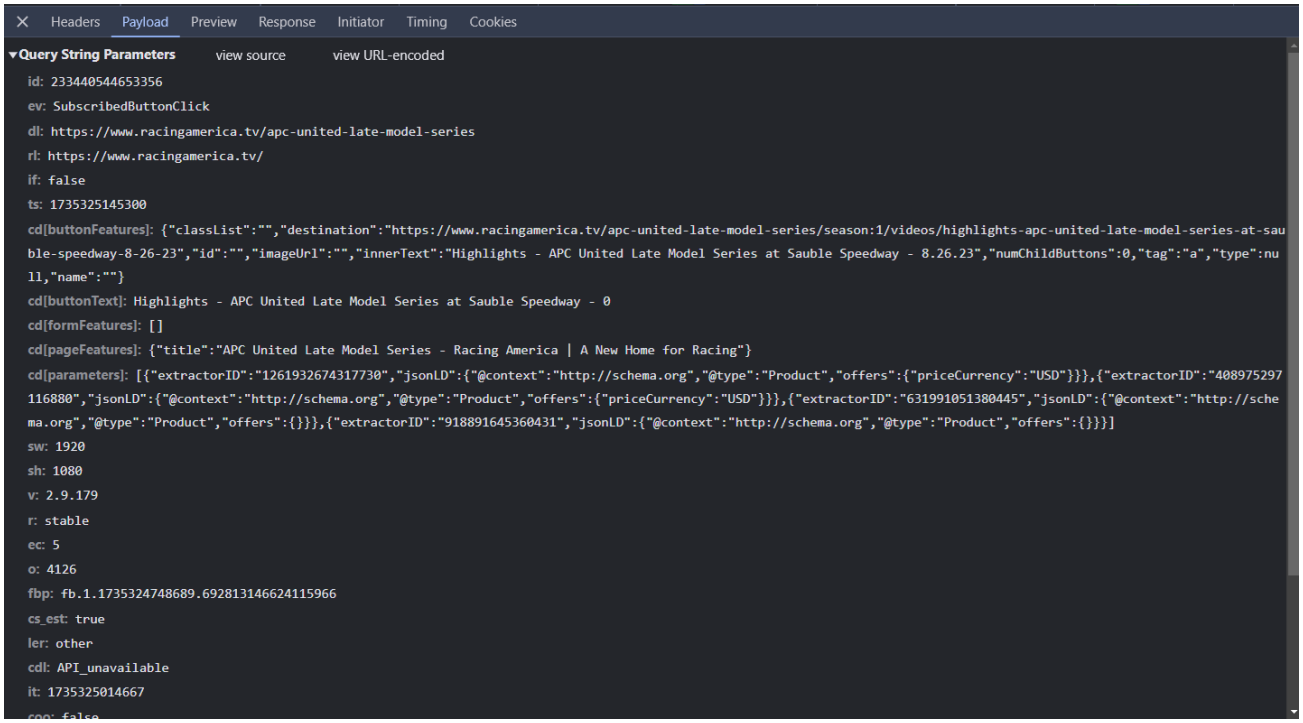

Figure 22 - Parsed URL Information from Sample Pixel Request

126. Similarly, the cookies attached to the Pixel's transmissions appear as a dense, albeit much less so, wall of text, as depicted below:

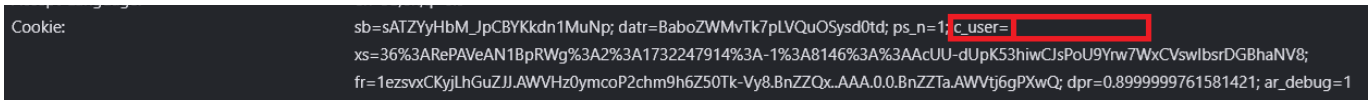

Figure 3 3- Cookie Data from Sample Pixel Request (c_user redacted)

127. However, like the URL data, the cookie data is easily parsed into more digestible format, as depicted below:

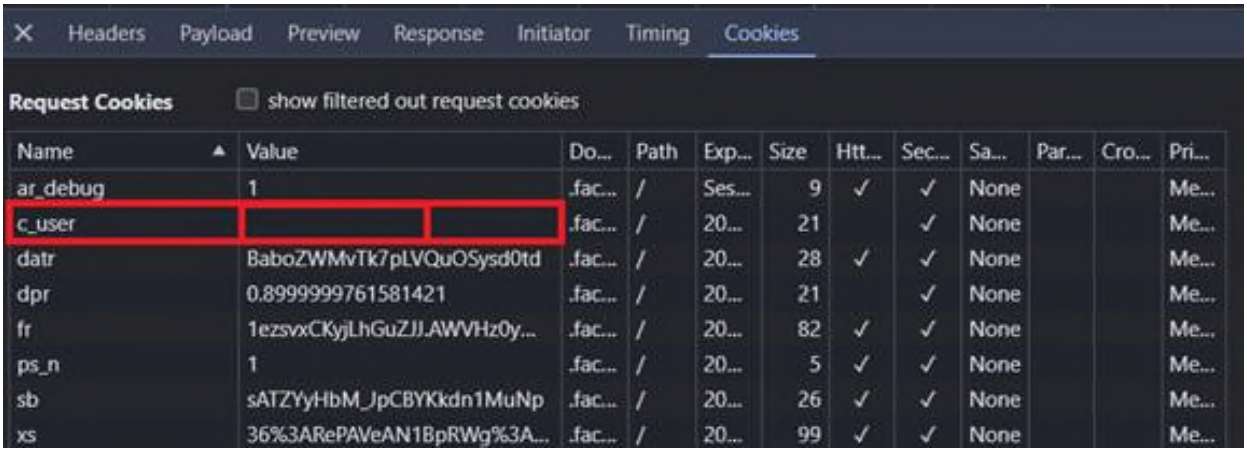

Figure 44 - Parsed Cookie Data from Sample Pixel Request (c_user redacted)

128. The c_user cookie can be used by anyone who receives the Pixel transmission to easily identify a Facebook user.

129. A c_user cookie contains a series of numbers (the UID) used to identify a specific profile, as depicted below:

Figure 5 5 - Sample UID number of test account created by Plaintiffs' counsel to investigate the Pixel, captured by a Pixel event

130. The information contained within the c_user cookie is considered PII. It contains "the kind of information that would readily permit an ordinary person to identify a specific

individual's video-watching behavior."[52] Because the UID can simply and easily be appended to "www.facebook.com/" to navigate to the relevant user's profile, it requires no special skill or expertise to identify the user associated with the UID, and courts have regularly upheld its status as PII.[53]

131. Any person, even without in-depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID. Using the UID from *Figure 5*, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the UID, as depicted below:

[52] *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 290 (3d Cir. 2016).
[53] *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

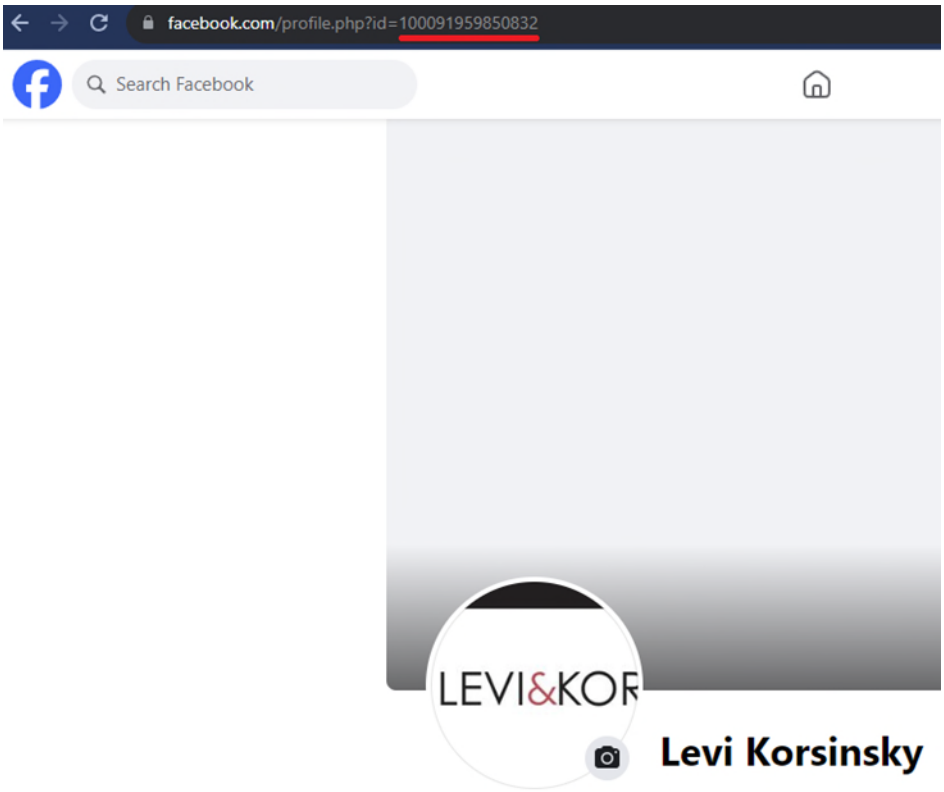

Figure 6 - Appending UID of a user to "facebook.com/" results in the user being redirected to the user's profile

132. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – are "always public."[54] No privacy setting on Facebook would allow Plaintiffs, or any user, to hide this basic information. By compelling a visitor's browser to disclose the c_user cookie alongside event data for media content, Racing America knowingly discloses information sufficiently permitting an ordinary person to identify an individual.

[54] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited Jan. 8, 2025).

3. The Pixel Shares Consumers' PII

133. The Pixel tracks user-activity on web pages by monitoring events,[55] which when triggered, causes the Pixel to automatically send data – here, Subscribers' PII – directly to Facebook.[56] Examples of events utilized by websites include: (i) a user loading a page with a Pixel installed (the "PageView event") [57] and (ii) when pre-designated buttons, like the "Watch" button, are clicked (the "SubscribedButtonClick" event).[58] The Website utilizes both.[59]

134. When a PageView and/or SubscribedButtonClick event is triggered, a "HTTP Request" is sent to Facebook (through Facebook's URL www.facebook.com/tr/).[60] This confirms that the Pixel events sent data to Facebook.

135. The HTTP Request includes a Request URL and embedded cookies such as the c_user cookie. It may also include information in its Payload,[61] such as metadata tags.

136. A Request URL, in addition to a domain name and path, contains parameters. Parameters are values added to a URL to transmit data and direct a web server to provide additional context-sensitive services, as depicted below:

Figure 7 – Mozilla's diagram of a URL, including parameters[62]

---

[55] *About Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Jan. 8, 2025).

[56] *See generally id.*

[57] *Specifications for Meta Pixel standard events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Jan. 8, 2025).

[58] *Reference: standard events*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/reference/ (last visited Jan. 8, 2025).

[59] The presence of Pixel events can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See About the Meta Pixel Helper*, FACEBOOK,

137. Defendant uses the Pixel as a Tracking Tool to collect and share Subscribers' PII with Facebook. Defendant does not disclose its data sharing practices or obtain permission from its Subscribers to share their PII with Facebook.

138. Defendant shares non-anonymized, PII and web watching history containing video titles with Facebook. Defendant's disclosures include unique identifiers (the UID) that correspond to specific Facebook users. The recipient finds the PII and web watching history packaged together in a single data transmission which is easily readable by an ordinary person once the PII is packaged and delivered by the Website's Tracking Tools.

139. Aside from using a paid subscription business model, Defendant monetizes the Website's Subscribers by disclosing Subscribers' PII to Facebook in a format which allows it to make a direct connection between the identity of a Subscriber and that Subscriber's PII, without the consent of its Subscribers and to the detriment of Plaintiffs' and Class Members' legally protected privacy rights.

140. Defendant had and continues to have the choice to design the Website so that the webpage URLs did not include the titles of videos. Defendant had, and has, the choice as to whether to purposefully include more information in the Website's URLs, including to improve

---

https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited Jan. 8, 2025).

[60] *How We Built a Meta Pixel Inspector*, THE MARKUP (Apr. 28, 2022 8:00 AM), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector.

[61] The "request payload" (or more simply, "Payload") is data sent by a HTTP Request, normally through a POST or PUT request, where the HTTP Request has a distinct message body. Payloads typically transmit form data, image data, and programming data. *See Request Payload Variation*, SITESPECT, https://doc.sitespect.com/knowledge/request-payload-trigger (last visited Jan. 8, 2025).

[62] *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Jan. 8, 2025).

website interaction and search engine optimization.[63] Here, Racing America chose to expose Subscribers' video information so that it could benefit from the tracking and sharing of Subscribers' PII.

141. Defendant also had the power to implement the Pixel in a way that shielded Subscribers' PII. Racing America chose, however, to transmit Subscribers' unencrypted PII.[64]

142. These factual allegations are corroborated by publicly available evidence. For instance, a Subscriber visits the Website, clicks on a pre-recorded video, such as "Highlights – APC United Late Model Series at Sauble Speedway – 8.26.23," and subsequently watches the video.

143. Sensitive data sent to Facebook through the triggered Facebook Pixel Events are included within the parameters of the Request URL, within the Request Header,[65] or as a Payload within the request. The specific Pixel Events implemented by Racing America sends Subscribers' PII through the Request URL parameters[66] and HTTP Headers.[67]

144. Defendant shares with Facebook the specific streaming content requested by Subscribers through Request URL parameters. Defendant also shares Subscribers' PII in the form

---

[63] *See* Chima Mmeje, *Domains*, MOZ (Nov. 11, 2024), https://moz.com/learn/seo/domain.

[64] *See Advanced Matching*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching (last visited Jan. 8, 2025).

[65] Request Headers are a subset of HTTP Headers that are used to provide information about a request's context, so that a server can customize its response to the request or supply authentication credentials to the server or otherwise provide more information about the client sending the request. *HTTP header*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/HTTP_header (last visited Jan. 8, 2025).

[66] URL parameters are values that are added to a URL to cause a web server to provide additional or different services. *What is a URL?*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Jan. 8, 2025).

[67] An "HTTP Header" is a field of an HTTP request or response that passes additional context and metadata about the request or response. *HTTP header*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/HTTP_header (last visited Jan. 8, 2025).

of an unencrypted and unique UID contained in the c_user cookie included in the HTTP Request Header, which can be used to find a user's personal Facebook page, as discussed in Section III(A)(2) above. This is portrayed in *Figures 8* through *10*, below.

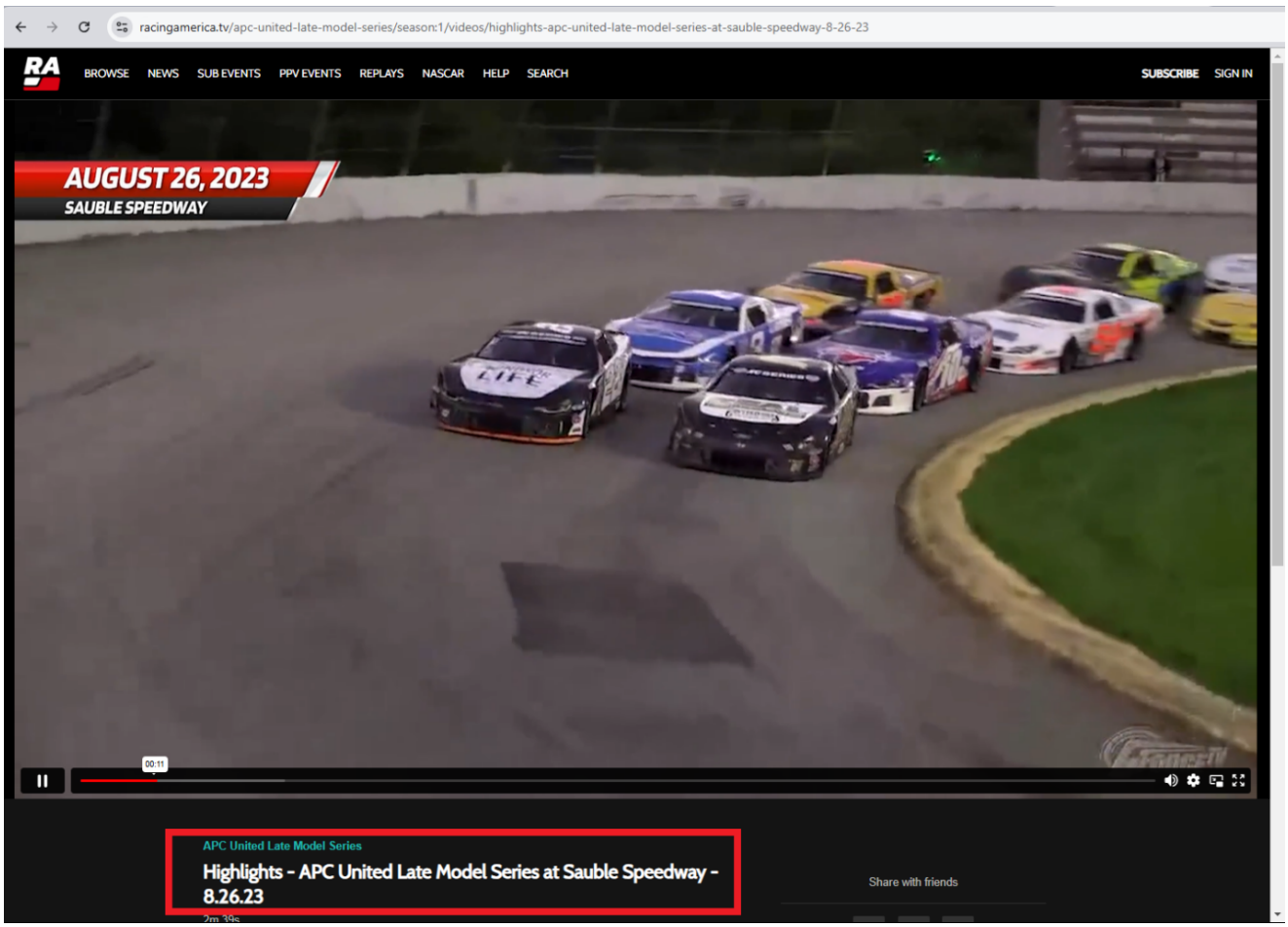

Figure 8 - Sample video webpage on the Website

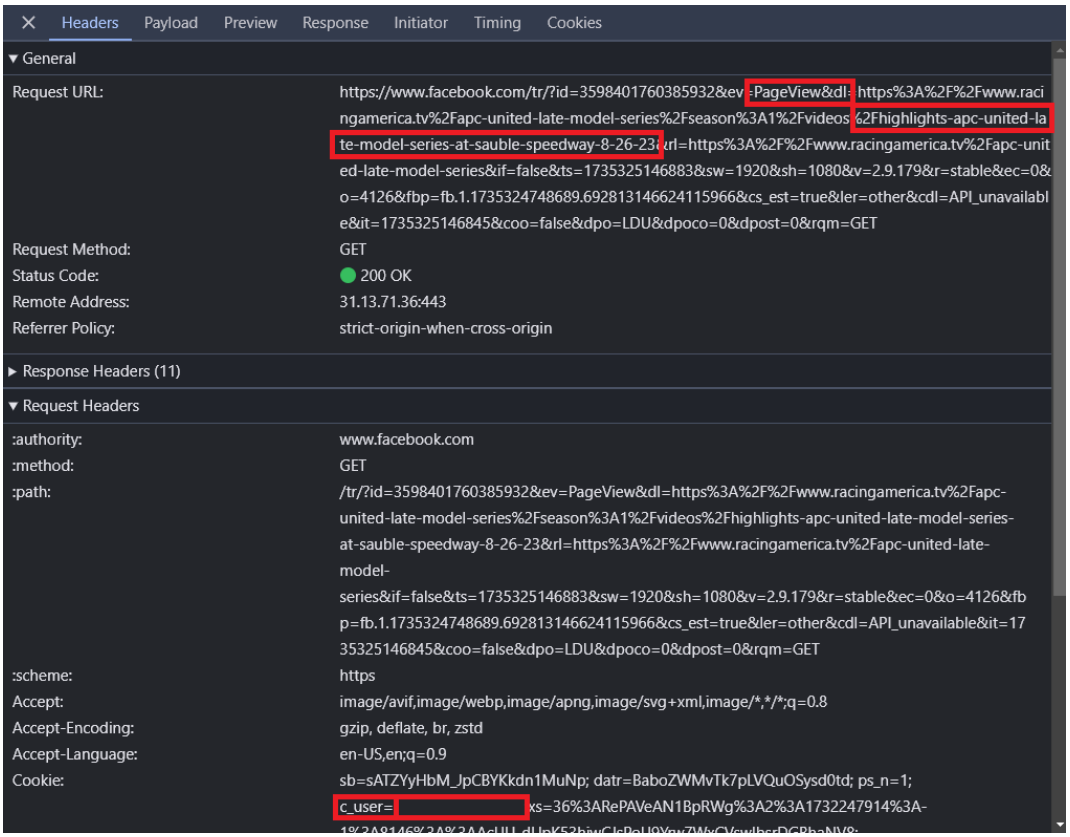

Figure 9 - Video Title and UID included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website

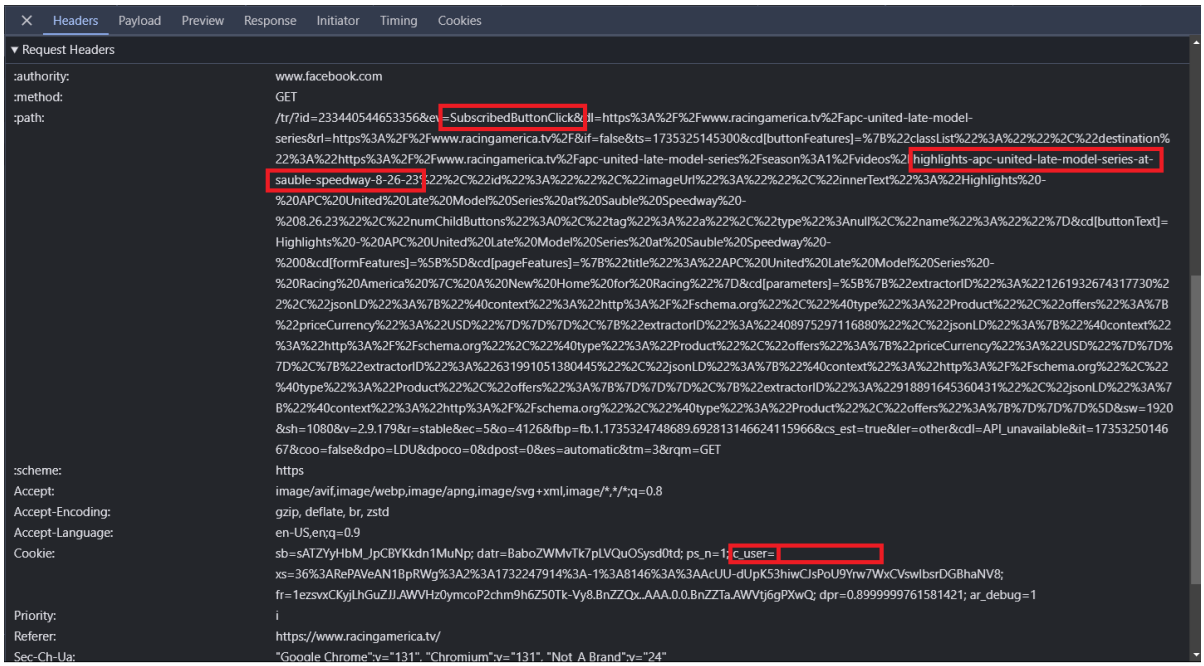

Figure 10 – Video Title and UID included in URL parameters disclosed to Facebook through SubscribedButtonClickPixel Event on the Website

4. The Pixel Shares Consumers' Search Terms

145. In addition to capturing and sharing Subscribers' video watching history (in violation of the VPPA) and irrespective of how the Subscriber reached the web watching page, the Pixel also intercepted and shared search terms entered by Plaintiffs.

146. For example, a search for "APC United Late Model Series" on the Website is depicted in *Figures 11* and *12*, below.

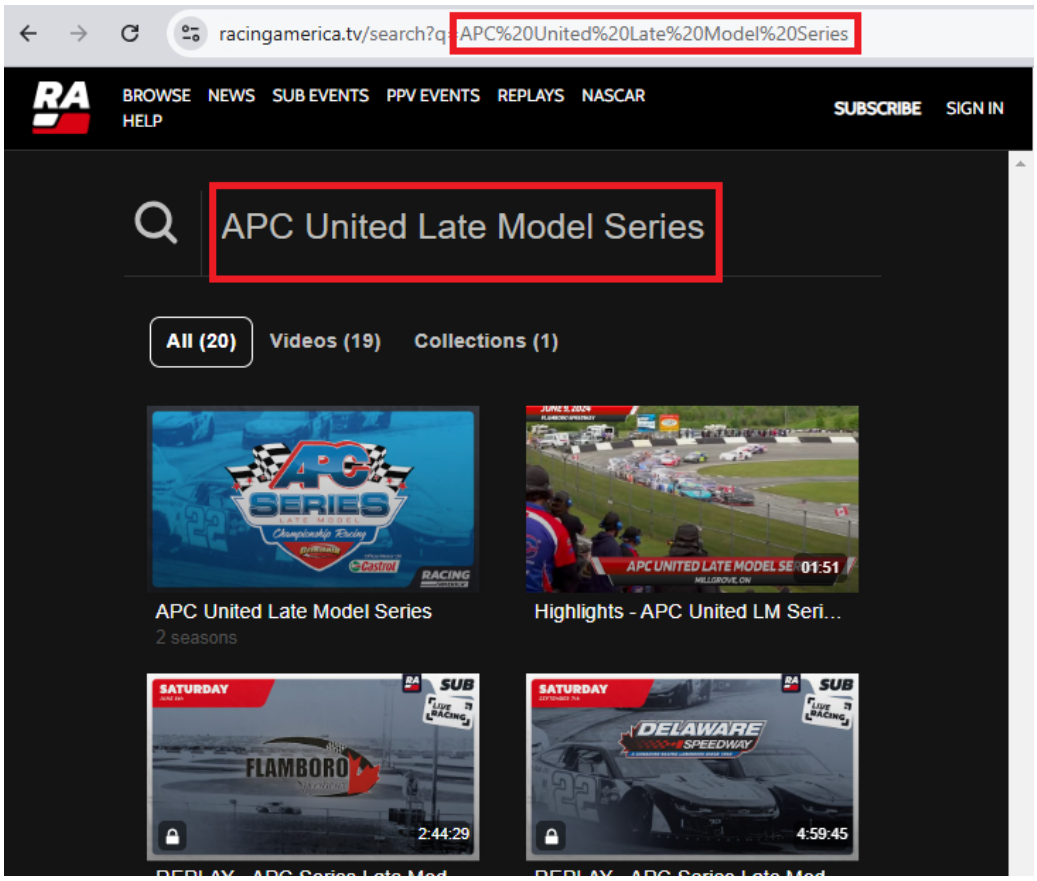

Figure 11 – Sample search for "APC United Late Model Series" on the Website

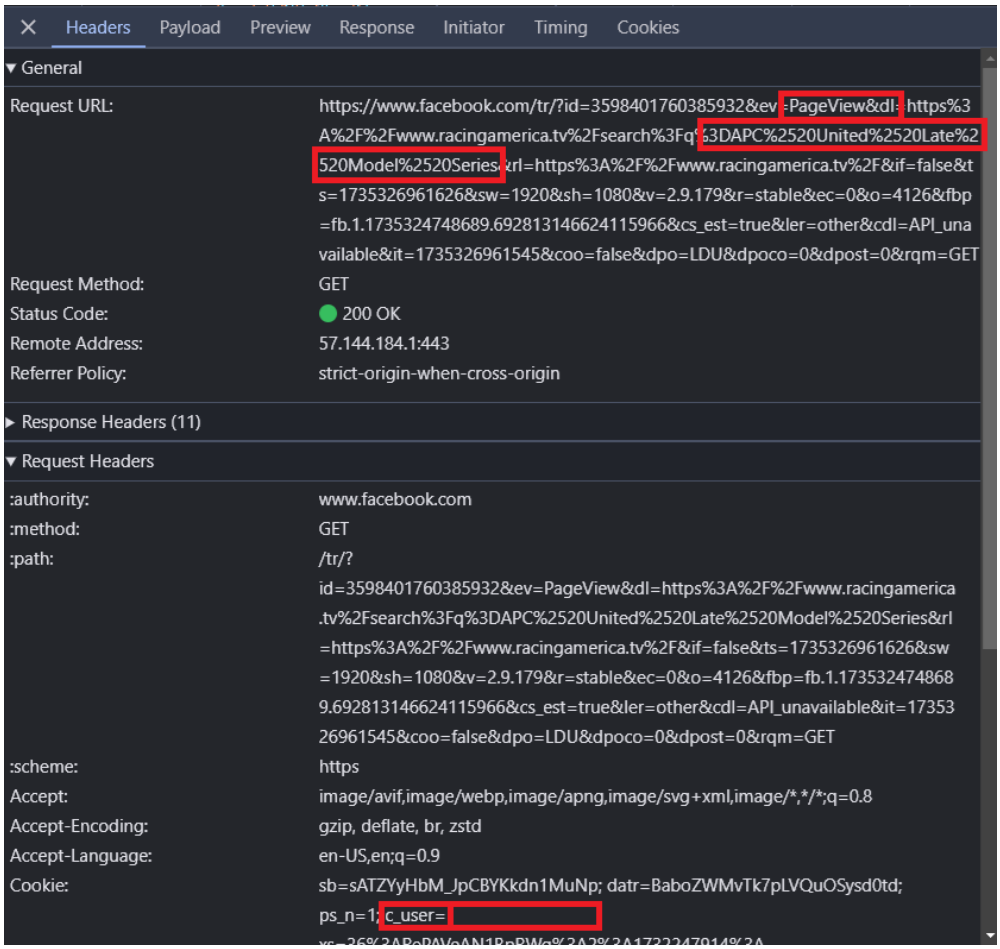

Figure 12 – Search terms and UID included and disclosed to Facebook through PageView Event

147. Such search terms, while independently confidential, may also include the capturing and sharing of searches associated with Subscribers' video watching history, resulting in violation of the VPPA.

148. The Pixel appears on the Website, as implemented by Defendant.

149. When a Subscriber or site visitor types and submits search terms into the search bar of the Website, those search terms are intercepted and monetized by Facebook.

150. Plaintiffs were unaware of the Pixel's intercepting of their confidential communications with the Website.

151. Plaintiffs reasonably believed that communications to the Website were made in confidence.

152. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to the Pixel's interceptions of Plaintiffs' search terms.

5. Defendant Was Told The Pixel Discloses Subscribers' Data; It Knew Precisely What the Pixel Would Collect and Share

153. When a business applies with Facebook to use the Pixel, it is provided with detail about its functionality (site policy) including PII.[68]

154. To make use of the Pixel, Defendant agreed to Facebook's Business Tool Terms (the "Business Terms").

155. The Business Terms informs website owners using Facebook's tracking tools that the employment of the Pixel will result in data sharing, including with Facebook, through the automatic sharing of Pixel Event information ("Event Data") and contact information ("Contact Information").[69]

156. The Business Terms are transparent that Meta will use the Event Data and Contact Information will be processed "solely to match the Contact Information against user IDs ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[70]

---

[68] *See Get Started*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/get-started (last visited Jan. 8, 2024) (The Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data . . . By default, the Pixel will track URLs visited [and] domains visited . . . .").

[69] *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Jan. 8, 2025).

[70] *Id.*

157. Facebook directs parties implementing the Pixel – here, Racing America – to encrypt request information[71] *before* data can be shared.[72]

158. Facebook further provides Pixel users, such as Racing America, guidance on responsible data handling, and details how data is acquired, used, and stored, including which information is shared with Facebook.

159. Facebook educates or reminds Pixel users of their responsibility to inform their subscribers of their website's data sharing, and specifically guides website owners to obtain the requisite rights, permissions, or consents, before sharing information with any third-party.[73]

160. As a sophisticated party entering into a business arrangement with another sophisticated party, Racing America was on notice of the potential privacy violations that would result from use of the Pixel, and ignored Facebook's warnings to safely handle its Subscribers' data and to warn its Subscribers that the Website would disclose information in a manner that threatened Subscribers' VPPA-protected PII.

B. The Google Tracking Tools

161. Google has an array of advertising products, each serving a specific function in advertising portfolios.

---

[71] This contrasts with Facebook's JavaScript Pixel, which automatically encrypts the data being sent. Racing America has specifically chosen the Pixel method which makes users' information visible. *See id.*

[72] *Id.*

[73] *Best practices for privacy and data use for Meta Business Tools*, FACEBOOK, https://www.facebook.com/business/help/363303621411154?id=818859032317965 (last visited Jan. 8, 2025).

1. Google Ads

162. One product, Google Ads (formerly AdWords), is an advertising platform developed by Google, that allows advertisers to place bids to display advertisements, service offerings, product listings, or videos to web users.[74]

163. The process advertisers using Google Ads to display ads within text-based search results is as follows: (i) advertisers create text-based ads with a title, description, and a link to the website to place within the Google search results; (ii) advertisers then choose keywords, usually related to their business or target audience, intended to trigger their ads to appear within the user's search results;[75] (iii) Google then allows advertisers to bid on those various keywords;[76] (iv) the advertiser with the highest bid wins the auction, and the ad is displayed on the search results page; and (v) the winning ad appears above or below the organic search results and is marked as an ad.

164. Google AdSense, works in conjunction with the Google Ads bidding system, allowing website owners to show Google Ads on websites and earn a revenue share from each ad each time it is viewed or clicked on their own sites.[77] The search terms that various entities bid for through Google Ads are then used by websites owners using Google AdSense to allow website owners to share in the profit Google generates from the advertising.

165. AdSense for content or AdSense for search are methods by which AdSense functions.[78] In either case, AdSense allows the website host to match ads to the website users based on the website's content and visitors.

166. Google Ads intercepted Plaintiffs' search terms, as depicted, below, using the sample search "APC United Late Model Series."

---

[74] *Achieve all your goals in one place*, GOOGLE ADS, https://ads.google.com/home/goals/ (last visited Jan. 8, 2025).

[75] *Reach the right people with Search ads*, GOOGLE ADS, https://ads.google.com/home/campaigns/search-ads/ (last visited Jan. 8, 2025).

[76] *Id*.

[77] *Home*, GOOGLE ADSENSE, https://www.google.com/adsense/start/how-it-works/ (last visited Jan. 8, 2025).

[78] *AdSense revenue share*, GOOGLE ADSENSE HELP, https://support.google.com/adsense/answer/180195?hl=en (last visited Jan. 8, 2025).

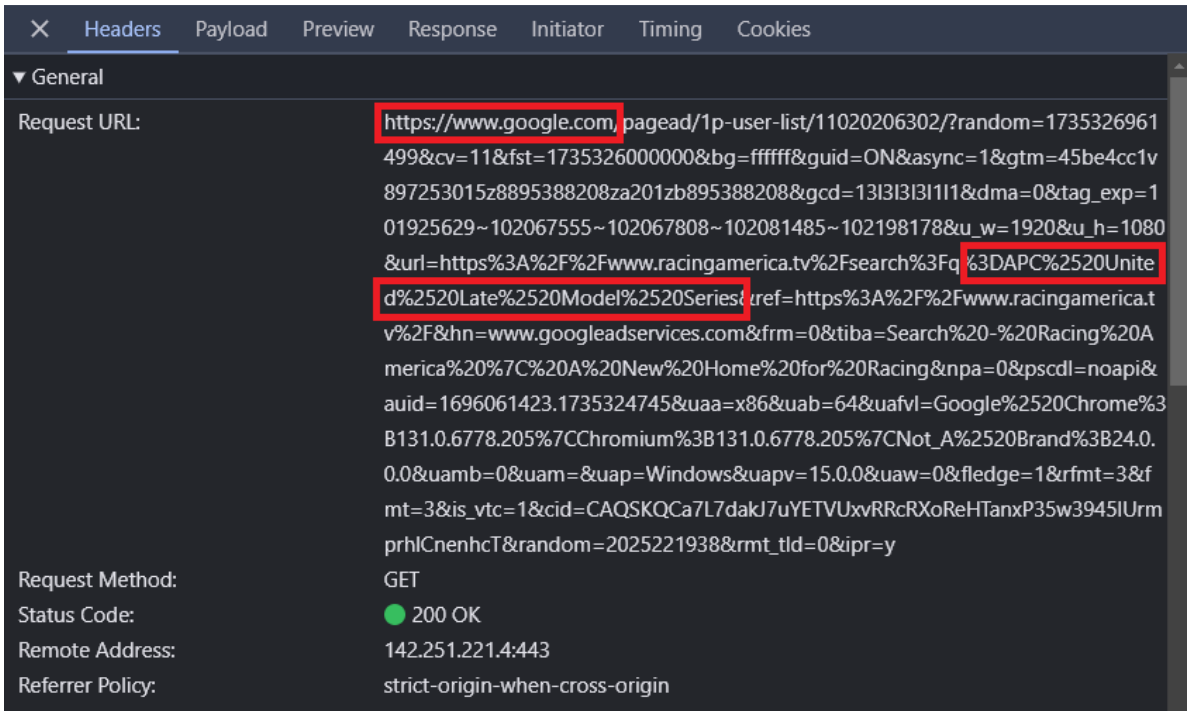

Figure 13 – Test search made on the Website resulted in sharing Search Terms with Google Page Ads

167. Google benefits when website owners utilize Google Ads and Google AdSense in connection with their websites.

168. Through Google AdSense, Google derives benefits from the ability to aggregate the search data it collects from website users to improve its own services and provide more relevant search results. By understanding patterns and trends in user behavior, Google better understands and gains unencumbered insight into what users are searching for and what they are interested in, which helps Google improve its own services, develop new products and overall increase revenues.

169. Google's collection and analysis of search results also allows it to improve its machine learning algorithms.[79] Google uses data on how users interact with search results to train its algorithms to provide more accurate and relevant search results.[80] For example, if a user clicks on a particular search result and spends more time on that page, Google learns that this page is

[79] Elle Poole Sidell, *What Does Google Do With Your Data?*, AVAST (Dec. 18, 2020), https://www.avast.com/c-how-google-uses-your-data.
[80] *Id.*

likely more relevant to that search query. By gathering this vast array of data on all users, Google can build an advertising portfolio for each user which includes their gender, age, job industry, and interests.[81]

170. Google profits in several ways from the Website's use of the Google search engine: (i) advertisers bid and pay Google for the keywords that will result in their ads showing in search results; (ii) through AdSense search, every time a user clicks or views an ad (depending on their chosen method), the advertiser will pay Google for that click or view; (iii) and Google's ability to aggregate user search data allows them to further tailor their own products to advertisers and users alike by training its algorithms with vast amounts of search data.

2. Google Analytics

171. Like the Facebook Pixel, Google Analytics ("GA") collects data about user interactions with a website, including: link clicks, button clicks, form submissions, conversions, shopping cart abandonment, adding items to carts, removing items from carts, file downloads, scrolling behavior, video views, call to action performance, table of contents clicks, and other customizable events.[82]

172. The data collected through GA is sent back to Google, which associates the activity with the website it was collected from.[83] Notably, Google notifies web developers that developers should provide "users with clear and comprehensive information about the data . . . collect[ed] on [their] websites" and to obtain "consent for that collection where legally required."[84]

---

[81] *Id.*
[82] Zach Paruch, *What Is Google Tag Manager & How Does It Work?*, SEMRUSH BLOG (Jan. 4, 2024) https://www.semrush.com/blog/beginners-guide-to-google-tag-manager/.
[83] *About the Google tag*, GOOGLE, https://support.google.com/tagmanager/answer/11994839?hl=en (last visited Jan. 8, 2025).
[84] *Id.*

173. In short, the use of GA represents specific data collection practices and settings and pre-determined destinations for that data. Google itself is aware of the potential legal violations its data collection tools are capable of, and puts the onus of warning users onto the website developers, such as Defendant.

174. Here, Defendant added GA to its Website, which resulted in the interception by and redirection of Plaintiffs' search terms to Google, as depicted from the example taken directly from the Website below.

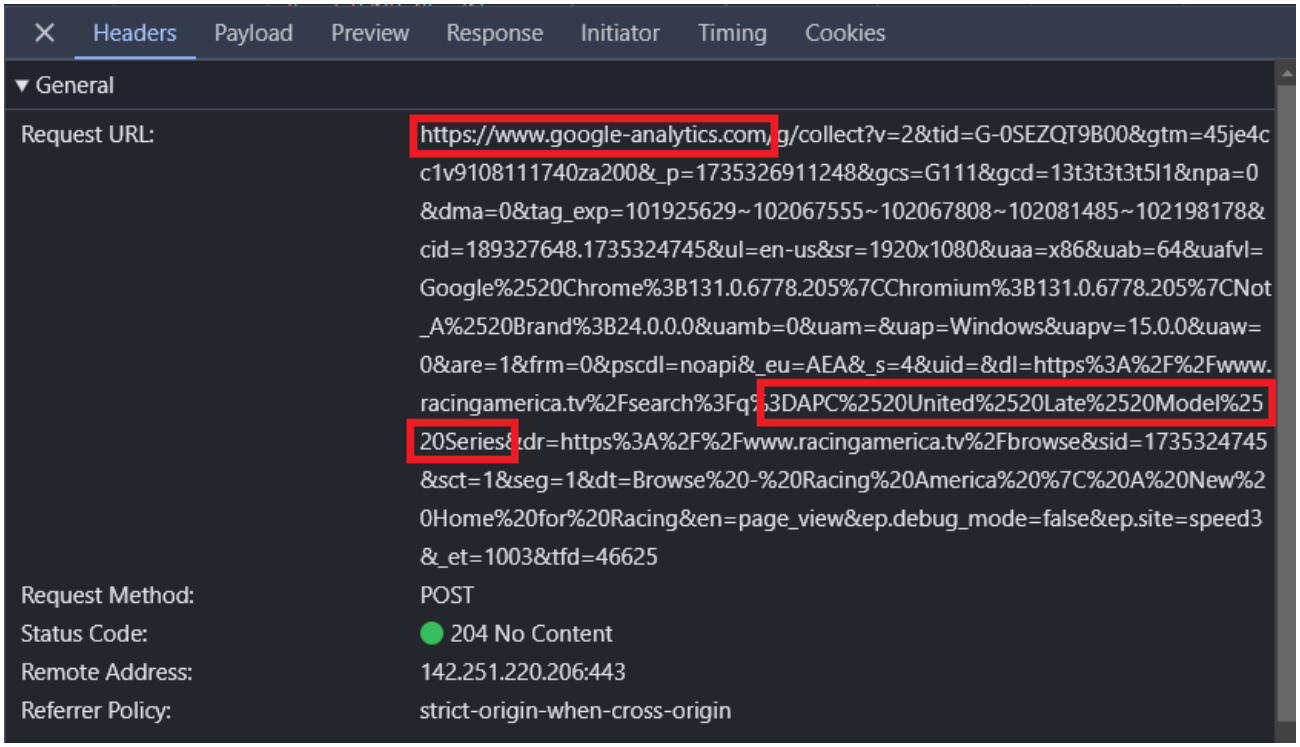

Figure 14 – Test search made on the Website resulted in sharing search terms with Google Analytics

175. After arriving at those common destinations, the Google products provide analysis and feedback which helps Defendant monetize the collected information through targeted advertising.

IV. The Website Lacks Informed, Written Consent Pursuant to the VPPA

176. The Website does not seek nor obtain permission from subscribers, including Plaintiffs and the Classes, to share Subscribers' PII or web watching history with third parties, including Facebook.

177. The sign-up process for the Website does not seek or obtain informed, written consent.

178. To the extent information about any of the Website's data sharing can be located, the language is not (i) presented to Subscribers of the site in a transparent manner, or where it must be viewed by visitors to the Website; (ii) made available as part of the sign-up process; (iii) offered to Subscribers as checkbox or e-signature field, or as any form of consent; and (iv) presented in terms that sufficiently warn Subscribers that their information, protected by the VPPA, will be shared with a third party.

V. Plaintiffs Did Not Consent to Defendant's Sharing of Plaintiffs' Search Terms

179. Plaintiffs were unaware of the Pixel's, and other Tracking Tools', interception of their confidential communications with the Website. The absent Class and Subclass Members were equally unaware of the Tracking Tools intercepting their confidential communications with the Website.

180. Plaintiffs reasonably believed that communications to the Website were made in confidence. Absent Class and Subclass Members held the same expectation in connection with their own communications between themselves and the Website.

181. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to the Tracking Tools' interceptions of Plaintiffs' search terms.

182. Meta and Google, by way of example, guide and caution website operators of the dangers of using their tracking tools without first providing notice of and then obtaining valid consent for invasively collecting consumers' protected data and either making that data available

to third-parties or allowing third parties to intercept consumers' protected information. Defendant agreed to these terms, in order to utilize and employ the Tracking Tools.

183. In contravention to Meta's and Google's terms and guidance, Plaintiffs were not given notice of the use of the Tracking Tools on the Website.

184. As a result, Plaintiffs did not and could not provide consent to the collection and sharing of their data when visiting the Website, running searches on the Website, and requesting videos from the Website.

VI. Plaintiffs Have a Privacy Right in their Search Terms

185. As Senator Leahy aptly foresaw, the time has come where companies can easily build profiles of customers based on their consumer habits.

186. Communications shared between consumers and companies appear to be private but, in reality, the contents of those messages are regularly shared.

187. Here, Defendant shares consumers' information, including search terms, with the Tracking Entities.

188. Search terms are inherently private. This is particularly true when the searches are communicated in confidence, or presumed to be private. All search terms are personal in nature, but there is an obviously heightened want for the searches to be kept confidential when the search terms themselves contain private information.

189. As described in Section I(A), descriptions and summaries of requested pre-recorded audio visual materials are private information worthy of federal protection.

190. Subscribers search for video materials on the Website using search terms. The search terms, when associated with descriptions or summaries of the pre-recorded videos, pertain to more than Subscribers' basic privacy.

191. Courts have recognized that users have a reasonable expectation of privacy in URLs that disclose unique search terms or the particular document within a website that a person views.[85]

192. As demonstrated in Section III, this private information is then shared with various third parties, including the Tracking Entities.

TOLLING

193. The statutes of limitations applicable to Plaintiffs' and the Classes' claims were tolled by Defendant's conduct and Plaintiffs' and Class and Subclass Members' delayed discovery of their claims.

194. As alleged above, Plaintiffs and members of the Classes did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiffs and members of the Classes could not have discovered Defendant's unlawful conduct with reasonable diligence.

195. Defendant secretly incorporated the Tracking Tools into the Website, providing no indication to Subscribers that their communications would be disclosed to these third parties.

196. Defendant had exclusive and superior knowledge that the Tracking Entities' Tracking Tools incorporated on its Website would disclose Subscribers' protected and private information and confidential communications, yet failed to disclose to Subscribers that by interacting with the Website, Plaintiffs' and Class and Subclass Members' PII would be disclosed to third parties.

[85] *Heerde v. Learfield Commc'ns, LLC*, No. 2:23-CV-04493-FLA (MAAX), 2024 WL 3573874 (C.D. Cal. July 19, 2024) (citing *Brown v. Google LLC*, 685 F.Supp.3d 909, 941 (N.D. Cal. 2023)).

197. Plaintiffs and members of the Classes could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the Tracking Entities' Tracking Tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website Subscriber that Defendant was disclosing and allowing the interception of such information to these third parties.

198. The earliest Plaintiffs and Class and Subclass Members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Complaint.

CLASS ACTION ALLEGATIONS

199. Plaintiffs bring this action individually and on behalf of the following Classes:

> **Nationwide Class**: All persons in the United States with a subscription to the Website that had their Sensitive Information improperly disclosed to third parties through the use of the Tracking Tools (the "Class").
>
> **Pennsylvania Subclass**: All persons in Pennsylvania with a subscription to the Website that had their PII improperly disclosed to third parties through the use of the Tracking Tools (the "Pennsylvania Subclass").

200. Specifically excluded from the Classes are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

201. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Classes should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

202. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

203. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Classes. However, given the popularity of Defendant's Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

204. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, subscribed to, and used, the Website to watch videos, and had their Sensitive Information collected and disclosed by Defendant.

205. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have no interests antagonistic to, nor in conflict with, the Classes. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

206. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class and Subclass Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class and Subclass Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

207. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and

fact common to the members of the Classes that predominate over questions that may affect individual members of the Classes include:

a. Whether Defendant collected Plaintiffs' and the Classes' Sensitive Information;

b. Whether Defendant unlawfully disclosed and continues to disclose the Sensitive Information of Subscribers of the Website in violation of the VPPA, the Federal Wiretap Act, and WESCA;

c. Whether Defendant's disclosures were committed knowingly; and

d. Whether Defendant disclosed Plaintiffs' and the Classes' Sensitive Information without consent.

208. Information concerning Defendant's Website's data sharing practices and subscription members is available from Defendant's or third-party records.

209. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

210. The prosecution of separate actions by individual members of the Classes would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

211. Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Classes as a whole.

212. Given that Defendant's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I

VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, *et seq*.
(On Behalf of Plaintiffs and the Class)

213. Plaintiffs hereby incorporate by reference and re-allege each and every allegation set forth above in all preceding paragraphs of this Complaint.

214. Plaintiffs bring this count on behalf of themselves and all members of the Class.

215. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d)." 18 U.S.C. § 2710(b)(1).

216. "Personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

217. A "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

218. Defendant violated this statute by knowingly disclosing Plaintiffs' and other Class Members' personally identifiable information to Facebook.

219. Defendant, through the Website, engages in the business of delivering video content to Subscribers, including Plaintiffs and the other Class Members, and other users. The Website delivers videos to subscribers, including Plaintiffs and the other Class Members, by making those materials electronically available to Plaintiffs and the other Class Members on the Website.

220. Defendant is a "video tape service providers" because it creates, curates, uploads, provides access to, sells access to, and causes the delivery of thousands of videos on the Website, thereby "engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

221. Defendant solicits individuals to pay to and/or subscribe to the Website.

222. Plaintiffs and members of the Class are "consumers" because they paid to subscribe to Defendant's Website. 18 U.S.C. § 2710(a)(1).

223. Plaintiffs and members of the Class viewed videos on the Website.

224. Defendant disclosed Plaintiffs' and Class Members' personally identifiable information to Facebook. Defendant utilized the Pixel which forced Plaintiffs' web browser to transmit Plaintiffs' identifying information, like their Facebook ID, along with Plaintiffs' and Class Members' event data, including the title of the videos they viewed, to Facebook.

225. Defendant knowingly disclosed Plaintiffs' and Class Members' PII, which is triggered automatically through Defendant's use of the Pixel. No additional steps on the part of Defendant, Facebook, or any third-party are required. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual to easily identify a Facebook user. *See* Section IIIA(2) (process to identify individual using UID).

226. Plaintiffs and members of the Class did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to Facebook. Defendant failed to obtain "informed, written consent" from subscribers – including Plaintiffs and members of the Class – "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and "at the election of the consumer," either "given at the time the

disclosure is sought" or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner." 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

227. Defendant's disclosures of Plaintiffs' and Class Members' PII were not made in the "ordinary course of business" as the term is defined by the VPPA. In particular, Defendant's disclosures to Facebook were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2). Instead, Plaintiffs' and Class Members' PII was used for improving marketing effectiveness.

228. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

229. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with VPPA's requirements for protecting a consumer's PII; (iii) statutory damages of $2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c); and (iv) reasonable attorneys' fees and costs and other litigation expenses.

COUNT II

VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § 2510, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

230. Plaintiffs hereby incorporate by reference and re-allege each and every allegation set forth in all preceding paragraphs of this Complaint.

231. Codified under 18 U.S.C. § 2510 *et seq.*, the Federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

232. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

233. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

234. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

235. The Wiretap Act defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

236. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

237. Defendant is a person for the purposes of the Wiretap Act.

238. The Pixel and other Tracking Tools constitute a "device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

239. The confidential communications Plaintiffs had with the Website, in the form of their Sensitive Information, were intercepted by the tracking entities and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

240. Plaintiffs had a reasonable expectation of privacy in their electronic communications with the Website in the form of their search terms submitted to the Website and browsing information. Even if Plaintiffs would not have had a reasonable expectation of privacy in the electronic communications normally, Plaintiffs' electronic communications with the Websites included descriptions and summaries of the films and/or videos they watched, searched for, requested, or subscribed to unlock access to, along with their identifying information, giving rise to a reasonable expectation of privacy pursuant to the VPPA.

241. Plaintiffs reasonably expected that third parties were not intercepting, recording, or disclosing their electronic communications with the Website.

242. Within the relevant time period, the electronic communications between Plaintiffs and the Website were intercepted by the Tracking Tools the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their PII, which includes the purpose of using such private information to develop advertising and marketing strategies.

243. Interception of Plaintiffs' confidential communications with the Website occur whenever a user uses the search bar within the Website and when navigating various webpages of the Website, including those containing videos.

244. At all times relevant to this complaint, Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Tracking Tools including that allowing the Tracking Tools to be implemented on the Website would cause the private communications of their Subscribers to be shared with the Tracking Entities.

245. Plaintiffs were never asked for their consent to expose their confidential electronic communications with Website to third parties. Indeed, such consent could not have been given

as Defendant never sought any form of consent from Plaintiffs to intercept, record, and disclose their private communications with the Website.

246. As detailed above, the Tracking Entities' unauthorized interception, disclosure and use of Plaintiffs' confidential communications were only possible through Defendant's knowing, willful, or intentional placement of the Tracking Tools on the Website. 18 U.S.C. § 2511(1)(a).

247. Plaintiffs have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such Plaintiffs are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and any profits made by the tracking entities as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (2) appropriate equitable or declaratory relief; and (3) reasonable attorneys' fees and other costs reasonably incurred.

COUNT III

VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTRAL ACT ("WESCA")
18 Pa. C.S.A. § 5701, *et seq.*
(On Behalf of Plaintiff Wambold and the Pennsylvania Subclass)

248. Plaintiff Wambold incorporates by reference and re-alleges each and every allegation set forth in all preceding paragraphs of this Complaint.

249. Plaintiff Wambold brings this claim individually and on behalf of the members of the proposed Pennsylvania Subclass against Racing America.

250. Racing America is a "person" as defined by 18 Pa. C.S.A. § 5702.

251. WESCA prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. 18 Pa. C.S.A. §§ 5701, 5703(1).

252. Racing America procured the Tracking Entities' services to "intercept" Plaintiff Wambold's and Pennsylvania Subclass Members' communications with Racing America, pursuant to WESCA, which defines "intercept" as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

253. Racing America subsequently used the contents of Plaintiff Wambold's communications with Racing America, intercepted and processed by the Tracking Entities, to target users with advertising, which is prohibited under WESCA. 18 Pa. C.S.A. § 5703(2)-(3).

254. WESCA also prohibits the knowing access to obtain access to a wire or electronic communication while it is in electronic storage by intentionally accessing, or exceeding the scope of access to, a facility through which an electronic communication service is provided. 18 Pa. C.S.A. § 5741(a)(1)-(2).

255. Racing America obtained Tracking Tools from the Tracking Entities to intercept and/or improperly access the communications between Racing America and its Subscribers in the conduct of its business, in violation of WESCA.

256. The devices used in this case, include, but are not limited to:

a. Racing America's own computers, which were used to add the Pixel to its webpages;

b. Racing America's servers used to host its webpages;

c. Plaintiff Wambold's and Pennsylvania Subclass Members' personal computing devices;

d. Plaintiff Wambold's and Pennsylvania Subclass Members' web browsers;

e. The Pixel itself;

f. Internet cookies;

g. Third-party code utilized by Racing America; and

h. Computer servers of third parties (including the Tracking Entities).

257. Defendant aided in the interception of communications between Plaintiff Wambold and Pennsylvania Subclass Members and Defendant that were subsequently redirected to and recorded by third parties without Plaintiff Wambold's or Pennsylvania Subclass Members' consent.

258. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed, or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

259. Plaintiff Wambold and the Pennsylvania Subclass members are Subscribers of Racing America's Website. Because Plaintiff Wambold and Pennsylvania Subclass Members plan to continue to use Racing America's Website in the future, if Racing America's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiff Wambold and Pennsylvania Subclass Members are likely to suffer continuing harm in the future.

260. Plaintiff Wambold and members of the Pennsylvania Subclass seek all relief available for violations of WESCA, including recovery of actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred, along with injunctive relief.

COUNT IV

INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Nationwide Class)

261. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in all preceding paragraphs of this Complaint.

262. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Racing America.

263. Racing America intentionally intruded upon Class Members' solitude or seclusion in that it effectively placed the Tracking Entities in the middle of conversations including Sensitive Information to which it was not an authorized party.

264. Racing America's participation in the Tracking Entities' tracking and interception of Sensitive Information were not authorized by Plaintiffs or Class Members.

265. Racing America's enabling of the Tracking Entities' intentional intrusion into Plaintiffs' and Class Members' internet communications including Sensitive Information was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individuals' privacy and against theft.

266. Secret monitoring of Sensitive Information is highly offensive behavior.

267. Wiretapping and the surreptitious recording of communications including PII is highly offensive behavior.

268. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is handling PII. Plaintiffs and Class Members have been damaged by Racing America's facilitation of Tracking Entities' intrusion upon their seclusion and are entitled to

reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

Injunctive Relief Of Defendant's Ongoing VPPA and Wiretap Violations

269. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative classes they seek to represent, and Defendant, which parties have a genuine and opposing interest in and which their interests are direct and substantial. Defendant has violated, and continues to violate, Plaintiffs' and Class Members' rights to protect their PII under the VPPA and the Wiretap Act.

270. Plaintiffs have demonstrated that they are likely to succeed on the merits of their claims, and are thus entitled to declaratory and injunctive relief.

271. Plaintiffs have no adequate remedy at law to stop the continuing violations of the VPPA and Wiretap Act by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the privacy rights of Plaintiffs, Class Members, and the absent Class Members, and will continue to cause, or allow to be caused, irreparable harm to Plaintiffs and Class Members. Injunctive relief is in the public interest to protect the Sensitive Information of Plaintiffs and Class Members, and other consumers that would be irreparably harmed through continued disclosure of their Sensitive Information.

272. Racing America completely disregards its obligation under the VPPA and Wiretap Act by loading the Tracking Tools onto the Website and facilitating the sharing of Subscribers' Sensitive Information with third parties for any ordinary person to access and use.

273. Despite brazenly violating the VPPA and the Wiretap Act, Subscribers were provided with no notice of the employment of the Tracking Tools and no indication of how or how much of their information was shared with third parties. Worse, in further violation of the VPPA and the Wiretap Act, Defendant did not seek or obtain any form of consent from

Subscribers for the use of the Tracking Tools to share information improperly pulled from the Website.

274. This threat of injury to Plaintiffs and members of the Class from the continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure their Sensitive Information is protected from future disclosure.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Classes and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

(d) Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to requiring Defendant to immediately (i) remove the Tracking Tools from the Website or (ii) add, and obtain, the appropriate consent from Subscribers;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) An award of statutory damages or penalties to the extent available;

(g) For Defendant to pay $2,500.00 to Plaintiffs and members of the Classes, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);

(h) For pre-judgment interest on all amounts awarded;

(i) For an order of restitution and all other forms of monetary relief;

(j) An award of all reasonable attorneys' fees and costs; and

(k) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: February 7, 2025

The Van Winkle Law Firm

By: */s/ David M. Wilkerson*

David M. Wilkerson
NC State Bar No. 35742
11 North Market Street
Asheville, NC 28801
(828) 258-2991
dwilkerson@vwlawfirm.com

Mark S. Reich*
Gary S. Ishimoto*
Alyssa Tolentino*
LEVI & KORSINSKY, LLP
33 Whitehall Street, Floor 17
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: gishimoto@zlk.com
Email: atolentino@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming